

# VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS

## PCT


### INTERNATIONALER VORLÄUFIGER BERICHT ÜBER DIE PATENTIERBARKEIT

(Kapitel II des Vertrags über die internationale Zusammenarbeit auf dem Gebiet des Patentwesens)

REC'D 12 OCT 2005

WIPO

PCT

Aktenzeichen des Anmelders oder Anwalts 2003P07731WO	<b>WEITERES VORGEHEN</b> siehe Formblatt PCT/PEA/416	
Internationales Aktenzeichen PCT/EP2004/050977	Internationales Anmeldedatum (Tag/Monat/Jahr) 01.06.2004	Prioritätsdatum (Tag/Monat/Jahr) 30.06.2003
Internationale Patentklassifikation (IPK) oder nationale Klassifikation und IPK G01C19/56, G01P21/00, B60T8/00, B60R21/01		
Anmelder SIEMENS AKTIENGESELLSCHAFT		
<p>1. Bei diesem Bericht handelt es sich um den internationalen vorläufigen Prüfungsbericht, der von der mit der internationalen vorläufigen Prüfung beauftragten Behörde nach Artikel 35 erstellt wurde und dem Anmelder gemäß Artikel 36 übermittelt wird.</p> <p>2. Dieser BERICHT umfaßt insgesamt 7 Blätter einschließlich dieses Deckblatts.</p> <p>3. Außerdem liegen dem Bericht ANLAGEN bei; diese umfassen</p> <p>a. <input checked="" type="checkbox"/> (an den Anmelder und das Internationale Büro gesandt) insgesamt 2 Blätter; dabei handelt es sich um</p> <p><input checked="" type="checkbox"/> Blätter mit der Beschreibung, Ansprüchen und/oder Zeichnungen, die geändert wurden und diesem Bericht zugrunde liegen, und/oder Blätter mit Berichtigungen, denen die Behörde zugestimmt hat (siehe Regel 70.16 und Abschnitt 607 der Verwaltungsvorschriften).</p> <p><input type="checkbox"/> Blätter, die frühere Blätter ersetzen, die aber aus den in Feld Nr. 1, Punkt 4 und im Zusatzfeld angegebenen Gründen nach Auffassung der Behörde eine Änderung enthalten, die über den Offenbarungsgehalt der internationalen Anmeldung in der ursprünglich eingereichten Fassung hinausgeht.</p> <p>b. <input type="checkbox"/> (nur an das Internationale Büro gesandt) insgesamt (bitte Art und Anzahl der/des elektronischen Datenträger(s) angeben), der/die ein Sequenzprotokoll und/oder die dazugehörigen Tabellen enthält/enthalten, nur in computerlesbarer Form, wie im Zusatzfeld betreffend das Sequenzprotokoll angegeben (siehe Abschnitt 802 der Verwaltungsvorschriften).</p>		
<p>4. Dieser Bericht enthält Angaben zu folgenden Punkten:</p> <p><input checked="" type="checkbox"/> Feld Nr. I Grundlage des Bescheids</p> <p><input type="checkbox"/> Feld Nr. II Priorität</p> <p><input type="checkbox"/> Feld Nr. III Keine Erstellung eines Gutachtens über Neuheit, erfinderische Tätigkeit und gewerbliche Anwendbarkeit</p> <p><input type="checkbox"/> Feld Nr. IV Mangelnde Einheitlichkeit der Erfindung</p> <p><input checked="" type="checkbox"/> Feld Nr. V Begründete Feststellung nach Artikel 35(2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung</p> <p><input type="checkbox"/> Feld Nr. VI Bestimmte angeführte Unterlagen</p> <p><input type="checkbox"/> Feld Nr. VII Bestimmte Mängel der internationalen Anmeldung</p> <p><input type="checkbox"/> Feld Nr. VIII Bestimmte Bemerkungen zur internationalen Anmeldung</p>		
Datum der Einreichung des Antrags  02.05.2005	Datum der Fertigstellung dieses Berichts  12.10.2005	
Name und Postanschrift der mit der internationalen Prüfung beauftragten Behörde   Europäisches Patentamt - P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tel. +31 70 340 - 2040 Tx: 31 651 epo nl Fax: +31 70 340 - 3016	Bevollmächtigter Bediensteter  Hoekstra, F  Tel. +31 70 340-3638	



# INTERNATIONALER VORLÄUFIGER BERICHT ÜBER DIE PATENTIERBARKEIT

Internationales Aktenzeichen  
PCT/EP2004/050977

## Feld Nr. I Grundlage des Berichts

1. Hinsichtlich der **Sprache** beruht der Bericht auf der internationalen Anmeldung in der Sprache, in der sie eingereicht wurde, sofern unter diesem Punkt nichts anderes angegeben ist.
- ☐ Der Bericht beruht auf einer Übersetzung aus der Originalsprache in die folgende Sprache, bei der es sich um die Sprache der Übersetzung handelt, die für folgenden Zweck eingereicht worden ist:
- ☐ internationale Recherche (nach Regeln 12.3 und 23.1 b))
  - ☐ Veröffentlichung der internationalen Anmeldung (nach Regel 12.4)
  - ☐ internationale vorläufige Prüfung (nach Regeln 55.2 und/oder 55.3)
2. Hinsichtlich der **Bestandteile\*** der internationalen Anmeldung beruht der Bericht auf *(Ersatzblätter, die dem Anmeldeamt auf eine Aufforderung nach Artikel 14 hin vorgelegt wurden, gelten im Rahmen dieses Berichts als "ursprünglich eingereicht" und sind ihm nicht beigelegt)*:

### Beschreibung, Seiten

1-6 in der ursprünglich eingereichten Fassung

### Ansprüche, Nr.

1-8 eingegangen am 02.05.2005 mit Schreiben vom 02.05.2005

### Zeichnungen, Blätter

1/1 in der ursprünglich eingereichten Fassung

☐ einem Sequenzprotokoll und/oder etwaigen dazugehörigen Tabellen - siehe Zusatzfeld betreffend das Sequenzprotokoll

3. ☐ Aufgrund der Änderungen sind folgende Unterlagen fortgefallen:
- ☐ Beschreibung: Seite
  - ☐ Ansprüche: Nr.
  - ☐ Zeichnungen: Blatt/Abb.
  - ☐ Sequenzprotokoll (*genaue Angaben*):
  - ☐ etwaige zum Sequenzprotokoll gehörende Tabellen (*genaue Angaben*):
4. ☐ Dieser Bericht ist ohne Berücksichtigung (von einigen) der diesem Bericht beigelegten und nachstehend aufgelisteten Änderungen erstellt worden, da diese aus den im Zusatzfeld angegebenen Gründen nach Auffassung der Behörde über den Offenbarungsgehalt in der ursprünglich eingereichten Fassung hinausgehen (Regel 70.2 c)).
- ☐ Beschreibung: Seite
  - ☐ Ansprüche: Nr.
  - ☐ Zeichnungen: Blatt/Abb.
  - ☐ Sequenzprotokoll (*genaue Angaben*):
  - ☐ etwaige zum Sequenzprotokoll gehörende Tabellen (*genaue Angaben*):

\* Wenn Punkt 4 zutrifft, können einige oder alle dieser Blätter mit der Bemerkung "ersetzt" versehen werden.

**INTERNATIONALER VORLÄUFIGER BERICHT  
ÜBER DIE PATENTIERBARKEIT**

Internationales Aktenzeichen  
PCT/EP2004/050977

---

**Feld Nr. V Begründete Feststellung nach Artikel 35 (2) hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung**

---

1. Feststellung
- |                                |                     |
|--------------------------------|---------------------|
| Neuheit (N)                    | Ja: Ansprüche 1-8   |
|                                | Nein: Ansprüche     |
| Erfinderische Tätigkeit (IS)   | Ja: Ansprüche       |
|                                | Nein: Ansprüche 1-8 |
| Gewerbliche Anwendbarkeit (IA) | Ja: Ansprüche: 1-8  |
|                                | Nein: Ansprüche:    |

2. Unterlagen und Erklärungen (Regel 70.7):

**siehe Beiblatt**

**Zu Punkt V**

**Begründete Feststellung hinsichtlich der Neuheit, der erfinderischen Tätigkeit und der gewerblichen Anwendbarkeit; Unterlagen und Erklärungen zur Stützung dieser Feststellung**

Es wird auf die folgenden Dokumente verwiesen:

- D1: US-A-5 839 096 (LYONS CHRISTOPHER T ET AL) 17. November 1998 (1998-11-17)
- D2: US 2002/178813 A1 (BABALA MICHAEL L) 5. Dezember 2002 (2002-12-05)
- D3: US-A-4727549 (TULPULE ET AL.) 23 Feb. 1988 (1988-02-23)

- 1 Die vorliegende Anmeldung erfüllt nicht die Erfordernisse des Artikels 33(1) PCT, weil der Gegenstand der Ansprüche **1-8** nicht auf einer erfinderischen Tätigkeit im Sinne von Artikel 33(3) PCT beruht. Die Begründung dafür ist die folgende:

**Neuheit:**

- 2.1 Dokument D1 offenbart: einen Sensor bei welchem ein Sensorelement und funktionalen Komponenten die Funktion des Sensors bewirken und ein Sensorausgangssignal erzeugen (Siehe D1, Sp. 6, Z. 14- 26 und Sp. 7, Z. 23-48 und Abb. 2; das Sensorelement besteht aus Transducervorrichtung 218 und Detektionsvorrichtung 222, die funktionalen Komponenten sind Zirkulator 236, Mixer 244, 250, 248, und Verstärker 262, 260, 258). Ein Sensorausgangssignal wird erzeugt und der Abstandsmessvorrichtung 224 zugeleitet. Diese funktionale Komponenten bilden eine Funktionssektion. Es sind weiter Kontrollkomponenten vorgesehen, die ausgebildet sind zur laufenden Kontrolle der funktionalen Komponenten (Sp. 6, Z. 32- 33 und Abb. 1, "system diagnostic" 11 mit "sub-diagnostics"; Siehe auch Sp. 6, Z. 67- Sp. 7, Z. 12). Weiter sind Überwachungskomponenten vorgesehen, zur Überwachung der Kontrollkomponenten mindestens einmal während eines Betriebszyklus (Sp. 7, Z. 13-20 und Sp. 18, Z. 32-61, der "watchdog timer" wartet auf ein Reset vom Mikroprozessor 194 während einer gewissen Periode, "a predetermined period of

time"). Der "watchdog timer" bildet eine Watchdog-Schaltung zur Überwachung des Mikrocomputers.

- 2.2 Laut PCT Richtlinien, Kapitel 5.40, hat das Merkmal "insbesondere einen Drehratensensor" keinen einschränkenden Effekt auf den Schutzzumfang des Anspruchs und ist daher als rein fakultativ zu betrachten.
- 2.3 Der Gegenstand des Anspruchs 1 unterscheidet sich daher von der aus D1 bekannten Einrichtung dadurch, daß die Überwachungssektion eine Komponente zur Überwachung des Takts eines in der Kontrollsektion enthaltenen Mikrocomputers, und eine Einrichtung zur Prüfung von Speichern innerhalb der Kontrollsektion enthält. Der Gegenstand dieses Anspruchs ist somit neu.
- 2.4 Ansprüche 2-8 sind vom Anspruch 1 abhängig und erfüllen damit ebenfalls die Erfordernisse des PCT in bezug auf Neuheit.

**Erfinderische Tätigkeit:**

- 3.1 In der D1 wird eine Kontrollkomponente, insbesondere der Mikroprozessor, überwacht von der Watchdog-Schaltung. Dem Fachmann auf diesem Gebiet ist es aber geläufig, daß sämtliche Komponenten der Kontrollsektion überwacht werden können und müssen. Es ist ihm weiter geläufig, daß bei Watchdogschaltungen der Takt des Mikrocomputers und auch die korrekte Wirkung der Speicher überwacht werden können. Für eine Illustration dieses allgemeinen Fachwissens, siehe D3, Sp. 1, Z. 18-30, Sp. 3, Z. 11-17 und Sp. 7, Z. 36-40. Der Gegenstand des unabhängigen Anspruchs 1 beruht somit nicht auf einer erfinderischen Tätigkeit.
- 3.2 Der Gegenstand der abhängigen Ansprüche 2 und 4 beruht ebenfalls nicht auf einer erfinderischen Tätigkeit, da die Merkmale dieser Ansprüche bekannt sind aus D1:  
Anspr. 2: Sp. 6, Z. 45- 52, "minimum level of noise".  
Anspr. 4: Sp. 6, Z. 52- 62.

- 3.3 Für den Anspruch 3 wird D2 als nächstliegender Stand der Technik angesehen. D2 offenbart eine Sicherheitseinrichtung für einen Drehratensensor mit Sensor (D2, Abb. 1 Vibrator 100), funktionalen Elementen (D2, Abb. 1, Sensorschaltkreis 200) und Kontrollkomponenten, die die funktionalen Komponenten kontrollieren (D2, Abs. [0030], [0033], Diagnoseschaltkreis 600 enthält Sensorkontrollschaltkreis 610, welcher das Sensorausgangssignal kontrolliert und vergleicht mit Schwellwertreferenzspannungen, d.h. Grenzwerten. Bei Störung gibt der Schaltkreis ein Diagnosesignal aus am Ausgang vom Schaltkreis 650, Siehe auch Abb. 2). Der Unterschied zwischen dem Gegenstand dieser Schrift und Anspruch 3 besteht in der Anwesenheit der Überwachungskomponenten, die die Kontrollkomponenten überwachen. Das Problem, welches dieses Merkmal zu lösen versucht, ist daß man bei der Diagnoseeinrichtung aus D2 bei Abwesenheit eines Störungsanwesenheitssignals am Ausgang vom Schaltkreis 650 oder sogar bei Anwesenheit eines Störungsabwesenheitssignals noch immer nicht sicher ist, daß alle Komponenten störungsfrei funktionieren, da ja die Diagnoseeinrichtung an sich defekt sein könnte.

Das technische Gebiet der Schrift D2 ist das der Fahrzeugtechnik. Es wird explizit das Fahrzeugbenehmen erwähnt. (Siehe Abs. [0012] und [0050]).

Der Fachmann sucht sich daher eine Lösung für das erwähnte Problem auf dem Gebiet der Fahrzeugsensoren. D1 hat das gleiche Problem und die gleiche Lösung wie Anspruch 3, nämlich die Überwachungskomponente (watchdog): die Taktüberwachung und Speicherüberwachung sind dem Fachmann geläufig, siehe Punkt 3.1 oben.

Der Fachmann würde das Merkmal aus D1 ohne erfinderisches Zutun auf die Einrichtung aus D2 anwenden und so zum Gegenstand des Anspruchs 3 gelangen. Dem Gegenstand dieses Anspruchs unterliegt daher keine erfinderische Tätigkeit.

- 3.4 Die verbleibenden Ansprüche 5-8 scheinen auch nicht erfinderisch zu sein: obwohl sowohl D1 als auch D2 Funktionssektionen mit ausschließlich analogen Komponenten beschreiben, ist das verwenden von digitalen Komponenten in solchen Schaltkreisen, und daher auch das Kontrollieren solcher Komponenten, eine

naheliegende Maßnahme (Anspr. 5-7). Das nicht mehrfach verwenden von Torschaltungen eines ASICs aus Sicherheitsgründen scheint an sich für den Fachmann naheliegend zu sein (Anspr. 8).

Neue Patentansprüche 1 bis 8

1. Sicherheitseinrichtung für einen Sensor, insbesondere einen Drehratensensor, bei welchem ein Sensorelement und funktionale Komponenten die Funktion des Sensors bewirken und ein Sensorausgangssignal erzeugen, wobei die funktionalen Komponenten (1, 10 bis 18) eine Funktionssektion (4) bilden, wobei ferner Kontrollkomponenten (19 bis 25) in einer Kontrollsektion (5) und Überwachungskomponenten (26, 27, 28) in einer Überwachungssektion (6) vorgesehen sind, wobei die Kontrollkomponenten (19 bis 25) zur laufenden Kontrolle der funktionalen Komponenten (1, 10 bis 18) ausgebildet sind, wobei die Überwachungskomponenten (26, 27, 28) zur Überwachung der Kontrollkomponenten (19 bis 25) mindestens einmal während eines Betriebszyklus ausgebildet sind und wobei die Überwachungssektion (6) eine Komponente (26) zur Überwachung des Takts eines in der Kontrollsektion enthaltenen Mikrocomputers, eine Watchdog-Schaltung (27) zur Überwachung des Mikrocomputers (19) und eine Einrichtung (28) zur Prüfung von Speichern innerhalb der Kontrollsektion (5) enthält.
2. Einrichtung nach Anspruch 1, dadurch gekennzeichnet, dass die Kontrollkomponenten (19 bis 25) zur Messung von Werten in der Funktionssektion (4) und zum Vergleich der gemessenen Werte mit Grenzwerten ausgebildet sind.
3. Einrichtung nach Anspruch 2, dadurch gekennzeichnet, dass die Kontrollkomponenten (19 bis 25) ferner zur Messung des Sensorausgangssignals und zum Vergleich des gemessenen Sensorausgangssignals mit Grenzwerten ausgebildet sind.
4. Einrichtung nach einem der Ansprüche 2 oder 3, dadurch gekennzeichnet, dass die Kontrollkomponenten (19 bis

- 25) ferner zu Tests der funktionalen Komponenten (1, 10 bis 18) ausgebildet sind, wobei Testsignale erzeugt und den funktionalen Komponenten (1, 10 bis 18) zugeführt werden und die Reaktion der funktionalen Komponenten (1, 10 bis 18) auf die Testsignale gemessen wird.
- 5
5. Einrichtung nach einem der Ansprüche 2 bis 4, dadurch gekennzeichnet, dass die Funktionssektion (4) Digital- (14 bis 17) und Analog-Komponenten (1, 10, 11) enthält und dass die Kontrollkomponenten zum Zugriff auf Register der Digital-Komponenten (14 bis 17) und zur Messung von Analogsignalen an den Analog-Komponenten (1, 10, 11) ausgebildet sind.
- 10
6. Einrichtung nach Anspruch 5, dadurch gekennzeichnet, dass die Kontrollsektion (5) eigene Analog-Komponenten (20 bis 23) und mindestens einen Analog/Digital-Wandler (24) enthält.
- 15
7. Einrichtung nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass die Überwachungskomponenten (26, 27, 28) im Wesentlichen zur Überwachung von digitalen Kontrollkomponenten (14 bis 17) ausgebildet sind.
- 20
8. Einrichtung nach einem der vorhergehenden Ansprüche, dadurch gekennzeichnet, dass Komponenten der Funktionssektion (4), der Kontrollsektion (5) und der Überwachungssektion (6) von einem anwendungsspezifischen integrierten Schaltkreis (ASIC) gebildet sind und dass in dem Schaltkreis enthaltene Torschaltungen jeweils nur einer der Sektionen zugeordnet sind.
- 25
- 30

**United States Patent** [19]  
**Tulpule et al.**

[11] **Patent Number:** 4,727,549  
[45] **Date of Patent:** Feb. 23, 1988

[54] **WATCHDOG ACTIVITY MONITOR (WAM)  
FOR USE WITH HIGH COVERAGE  
PROCESSOR SELF-TEST**

[75] **Inventors:** Bhalchandra R. Tulpule, Vernon;  
Richard W. Crosset, III, Simsbury;  
Richard E. Versailles, New Hartford,  
all of Conn.

[73] **Assignee:** United Technologies Corporation,  
Hartford, Conn.

[21] **Appl. No.:** 758,251

[22] **Filed:** Sep. 13, 1985

[51] **Int. Cl.<sup>4</sup>** ..... G06F 11/00

[52] **U.S. Cl.** ..... 371/62; 371/25

[58] **Field of Search** ..... 371/15, 25, 62;  
324/73 R, 73 AT, 73 PC

[56] **References Cited**

**U.S. PATENT DOCUMENTS**

3,749,897	7/1973	Hirvela	371/62 X
3,919,637	11/1975	Earp	371/25
4,161,276	7/1979	Sacher et al.	371/25
4,176,780	12/1979	Sacher et al.	371/25
4,392,226	7/1983	Cook	371/61
4,410,938	10/1983	Higashiyama	371/62 X
4,594,685	6/1986	Owens	371/62 X

4,635,258 1/1987 Salowe ..... 371/62 X

**OTHER PUBLICATIONS**

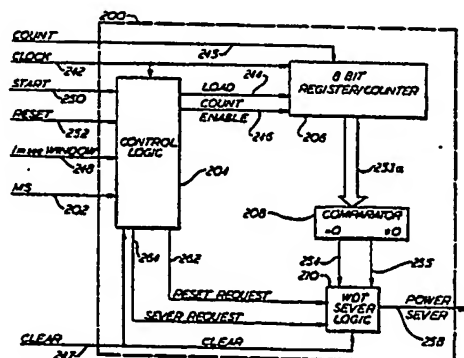
J. P. Hayes, Transition Count Testing of Combinational Logic Circuits, *IEEE Trans. on Computers*, vol. C-25, No. 6, Jun. 1976, pp. 613-620.

*Primary Examiner*—Charles E. Atkinson  
*Attorney, Agent, or Firm*—Francis J. Maguire, Jr.

[57] **ABSTRACT**

A high fault coverage, instruction modeled self-test for a signal processor in a user environment is disclosed. The self-test executes a sequence of sub-tests and issues a state transition signal upon the execution of each sub-test. The self-test may be combined with a watchdog activity monitor (WAM) which provides a test-failure signal in the presence of a counted number of state transitions not agreeing with an expected number. An independent measure of time may be provided in the WAM to increase fault coverage by checking the processor's clock. Additionally, redundant processor systems are protected from inadvertent unsevering of a severed processor using a unique unsever arming technique and apparatus.

**13 Claims, 8 Drawing Figures**



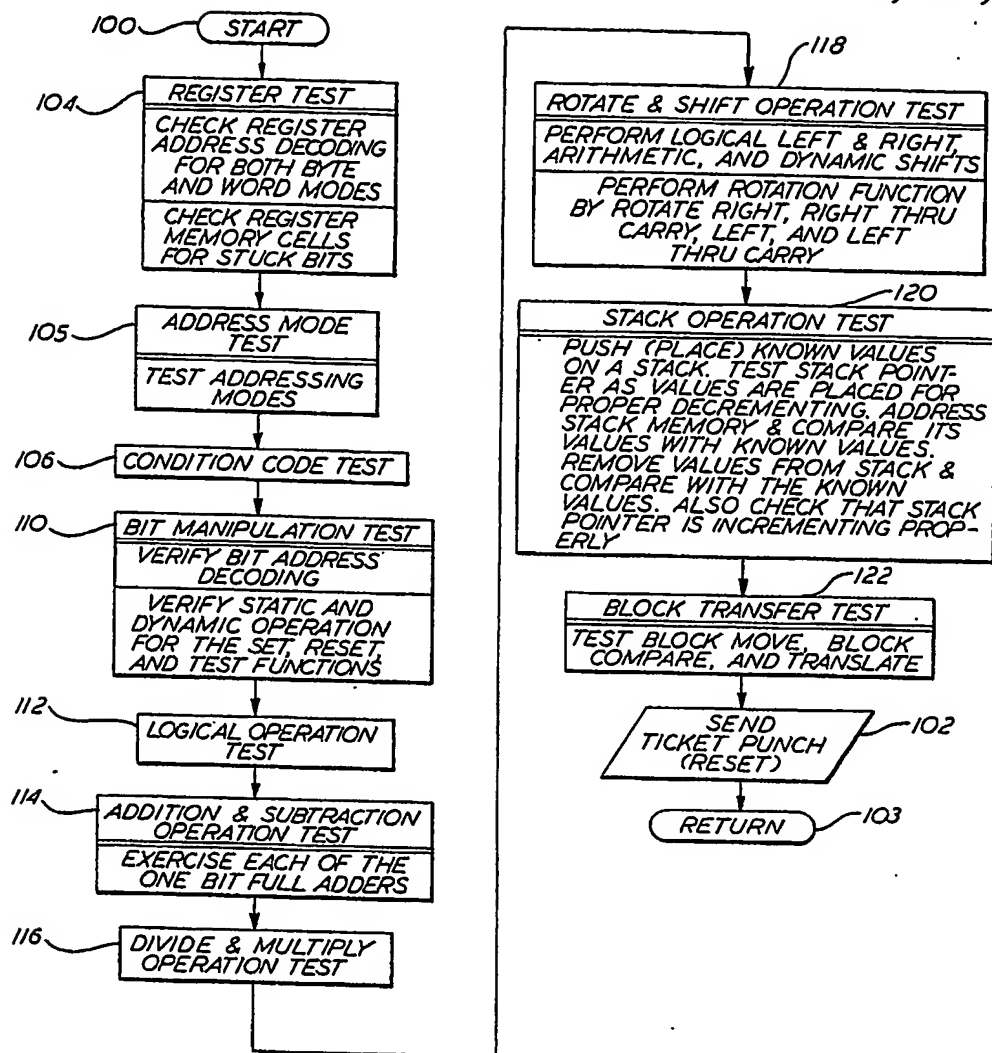


FIG. 3

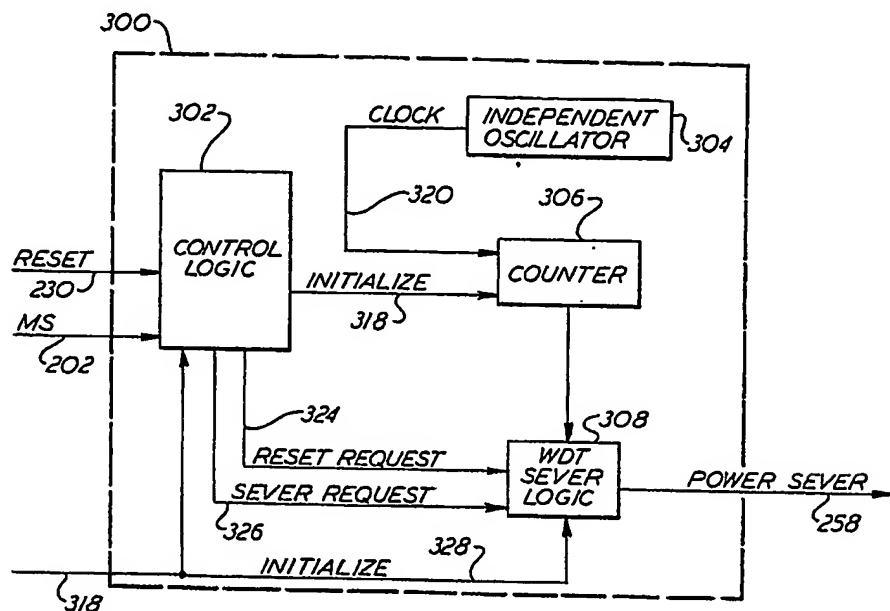


FIG. 6

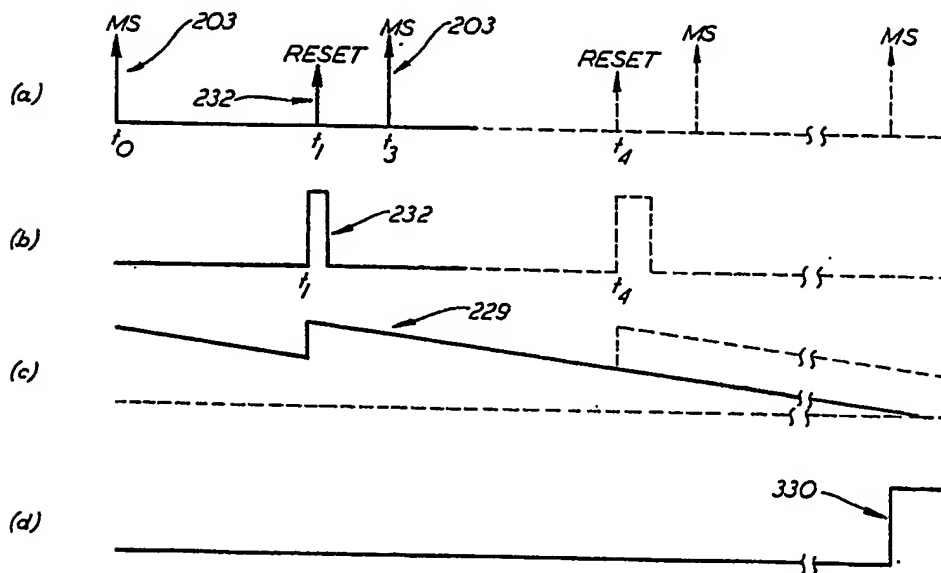


FIG. 7

## WATCHDOG ACTIVITY MONITOR (WAM) FOR USE WITH HIGH COVERAGE PROCESSOR SELF-TEST

The invention described herein was made in the performance of work under NASA Contract No. NAS2-11771 and is subject to the provisions of Section 305 of the National Aeronautics and Space Act of 1958 (72 Stat. 435; 42 U.S.C. 2457).

### TECHNICAL FIELD

This invention relates to detecting signal processor faults in a user environment with a high degree of fault coverage and to predicting that fault coverage.

### BACKGROUND ART

In many digital computer systems the detection and correct isolation or "coverage" of failures in the computer is a matter of great concern. This is particularly true in avionic type computer systems such as flight, engine, navigation or weapon control systems where redundant control systems exist and the correct isolation of a fault must be guaranteed with a high probability without regard to the source of failure. Upon detection of a fault one of the redundant systems is immediately selected to "carry" the system. A variety of Built-In-Test (BIT) techniques have been developed to meet such requirements. Notable among these are the Watchdog Timer (WDT) function and processor self-tests.

The WDT function, also known as "ticket punch" or "sanity monitor" is used to monitor correct software operation by requiring periodic updating or resetting of the WDT hardware within a legal time interval known as a window. This WDT function is a "non-specific" monitor which can detect any selected failure that can cause the program to diverge from its correct execution sequence and thereby miss the WDT update window. The particular implementation of a WDT function can sometimes erode its coverage capability. For example, if the WDT window is too large and the WDT can be updated more than one time within the window, the coverage probability for, say, a program looping failure is thereby reduced.

The processor self-test, unlike the WDT, is a very specific test involving a collection of specific "must work" instructions for a given processor. The tests are executed using specific data as inputs and are designed to "exercise" the maximum number of individual gates in the processor. Clearly this is a formidable task even for the simplest microprocessors due to the essentially infinite number of possible machine states. A very large proportion of these must be tested to assure a high degree of coverage.

The coverage provided by processor self-tests is generally very difficult to predict and has been the subject of many studies. See, for example, an article by Thatte, S. M. and J. A. Abraham, "Test Generation for General Microprocessor Architectures," in *IEEE Proc. of 1979 International Symposium on Fault-Tolerant Computing*, Madison, Wisc., IEEE Computer Society, pp. 203-210, June, 1979. There, a graph-theoretic model for microprocessor architecture is presented which permits the treatment of the organization and instruction set as parameters of test generation procedures. Functional level fault models for the register decoding function, and the instruction decoding and control function are developed independent of the details of implementation.

Test generation procedures are presented to detect faults in these functions. Their approach is potentially attractive in a user environment because it suggests the avoidance, to some extent, of the normally enormous amount of computation required to generate test sets for the very large number of gates, flip-flops, and interconnections in LSI circuits such as microprocessors.

In the past, when faced with this task, semiconductor and sometimes system manufacturers have resorted to exhaustive testing of each and every machine state and stuck-at fault condition. However, this approach is unsuitable for providing real time, on line, built-in-test (BIT) coverage of avionic computer systems because of the size of the test.

One of the most important drawbacks of these tests is that they lack an independent, external monitor for the execution and correct completion of these self-tests. In the absence of such a monitor function, such as a WDT, there would be no assurance that the self-test was ever started or successfully completed. The monitoring hardware must be independent of the processor so that the use of the processor under test as a monitor would defeat the purpose of the test.

### DISCLOSURE OF INVENTION

The object of the present invention is to provide a highly reliable method and apparatus for the on-line, real time, detection and isolation, i.e., "coverage", of internal failures in a digital computer which may be used to guarantee channel shutdown to a very high degree of certainty in the presence of such failures.

According to a first aspect of the present invention, an instruction modeled self-test method is combined with a Watchdog Activity Monitor (WAM) which must be periodically started and then stopped at the precise time that each self-test is completed in order to avoid having the WAM initiate a trip out or cause a channel sever action. During each WAM activity monitoring interval, the CPU under test executes a processor self-test; the CPU issues a sequence of state transition signals after each subtest is completed; the failure to complete the test, as measured by the number of transition signals received, exactly at the end of the interval, as indicated by a reset signal provided by the CPU, results in a guaranteed WAM trip leading to channel sever. The concept of encompassing a comprehensive functional processor self-test with the WAM function to provide a very high and predictable coverage of processor faults is at the center of this invention.

It is essential, in order to understand the central teaching of this first aspect of the present invention, to understand that the timing aspects of the WDTs of the prior art have been abandoned in the WAM of the present invention. The processor self-test is set-up in advance to test the major functional blocks of the signal processor. These may include bit manipulation tests, logical operation tests, addition and subtraction operational tests, divide and multiply operational tests, and rotate and shift operational tests. Of course, a variety of these tests may be excluded and other tests may be included. At the conclusion of each of the above major categories of tests a transition is made to the next major category of tests. At that time, a transition signal is sent into the Watchdog Activity Monitor indicating that one of the major tests has been completed. Of course, transition signals could be sent more frequently, at the conclusion of minor test steps accomplished within each major functional test block. Each time that the WAM

the expected count, the channel will be severed by the WAM. The best mode embodiment disclosed herein utilizes a counter responsive to the above described count pulses. If the counter counts down to zero before or after expected, a channel sever is initiated. It should of course be understood that many other similar approaches may be taken in implementing the tracking of the state transitions of the self-test.

The state transitions in the Markov diagram of FIG. 1 are probabilistic in nature with the probability of taking incorrect paths denoted by  $P_F$ , i.e., the probability of a failure. The  $P_F$  values are assumed to be the same for all state transitions for the sake of simplification.

In terms of the Markov model, the processor self-test described in this invention can be described as a finite state machine that transitions sequentially from the initial state  $Q_0$  through states  $Q_1, Q_2, \dots$  to the final state  $Q_N$  without any deviation. The associated WAM in this scheme is a counter which counts the correct number of state transitions. More sophisticated counting schemes that distinguish between the various types of transitions, i.e., instruction types, are possible, and are entirely within the scope and intent of the present invention. However, the simplified approach illustrated here is adequate to establish the concepts required to achieve minimum coverage by the WAM as taught herein. In any case, regardless of the counting mechanism used, whenever an incorrect number of state transitions are detected by the WAM at the end of a particular test execution, this leads to channel sever.

The probability of correct failure detection and isolation, i.e., "coverage" (C) can be calculated as follows. The lack of coverage (1-C) can be attributed to those sequences of incorrect state transitions through state  $Q_F$  for which the total number of state transitions appears to be correct so that the WAM is unable to detect the failure. As may be seen from FIG. 1, there are many paths for which this is possible. One such sequence is a failure sequence  $Q_0, Q_1, Q_F, (N-3) Q_F, Q_N$  in which (N-3)  $Q_F$  denotes that exactly N-3 transitions from  $Q_1$  to state  $Q_F$  take place before  $Q_N$  is reached with a total of N transitions and the WAM is not tripped. The total probability of the lack of coverage can therefore be given by:

$$1 - C = \sum_{i=1}^N P_F^2 (1 - P_F)^{N-2} \\ = N \cdot P_F^2 (1 - P_F)^{N-2}.$$

Thus for a processor with  $P_F = 10^{-5}$  (10 failures per  $10^6$  hours), a 100 state WAM gives a lack of coverage of

$$1 - C = 100 \times 10^{-10} (1 - 10^{-5})^{98} \\ = 9.99 \times 10^{-10}$$

so that

$$\text{coverage (C)} = 0.9999999991 = 0.991$$

Of course it will be understood that the above calculation assumed that every processor failure is detected by the WAM self-test. This is usually not true because of the large number of gates and their possible failure modes. A variety of techniques have been developed in the prior art, the best known of them being the stuck-at gate fault models. The task of simulating stuck-at gate faults to determine the coverage capability of a self-test

is extremely difficult because of the extremely large number of possible failure modes of a complex processor. A more powerful technique has been developed by Thatte and Abraham who have modeled the processor architecture in terms of the instructions and registers (see their article referred to in the Background Art section). Their approach deals with failures in instruction or data path execution and is therefore independent of the specific gate level implementation.

The self-test design methodology used in this invention is different from that approach in that it is based on a functional model of the processor such as the model shown in FIG. 2. The modules or elements in the processor are conventional or classical such as registers, arithmetic and logic units, multipliers, rotate and shift units, comparators, instruction decoder, etc., all connected with data and address bus connections for external connection. The method is general enough so that new or unconventional elements can be added to the processor model. In any case, the gate level implementation of these elements is analyzed to determine the apportionment of the processor failure rate. The tests are then developed to exercise each type of instruction and the percentage of failures that can be covered by each test is determined. For example, a shift and rotate unit might be tested by testing right and left shifts for specified logical and arithmetic operands and comparing against expected results. As another example, all gates associated with an adder can be checked by adding one to the largest binary number represented and checking for an overflow with zero as a result. The data input for the tests are chosen to maximize the number of gates that are energized by the test.

The block diagram illustration of FIG. 2 is a functional model of a signal processor 50 including registers 52, ALU 54, program counter 56, control unit 58, interrupt control 60, and address/timing 61 functional blocks. Of course, the typical signal processor will also include other major functional blocks which are not included for the sake of simplicity. Each of the functional block may be conceptualized as communicating with a data bus 62, an address bus 64, and a control bus 65.

FIG. 3 is an illustration of a comprehensive test procedure which may be carried out on a processor modeled according to the functions which it is capable of carrying out as, for example, in FIG. 2. Thus, the test procedure illustrated in FIG. 3 is designed for specific use on a typical signal processor. It will therefore be appreciated that the WAM of the present invention is not restricted to use with any particular processor or to a particular test sequence. The processor test sequence described herein is merely illustrative of one of many such tests which may be practiced according to the present invention. The CPU self-test of FIG. 3 is designed to test the processor for hardware faults using the machine instruction set. Each test checks a specific microprocessor function with the assumption that all other functions of the processor are working and are tested elsewhere. The union of the fault coverage of all the tests approaches 100% coverage.

The CPU self-test is performed periodically in order to provide a ticket-punch signal to a Watchdog Activity Monitor (WAM) each time the series of tests is successfully executed. The WAM hardware will be described in detail later; but first, a summary outline of a typical

tests may be designed to rotate single as well as multiple bits in one instruction.

The self-test next executes, in a step 120, a stack operation available in most processors today. A push operation is used to place known values on a stack. As the values are placed on the stack, the stack pointer is tested to assure it is decremented correctly. The memory of the stack is then addressed and its values compared with the known values. Next the values are removed from the stack using the pop operation. As the values are removed, they are compared with the known values and the stack pointer is tested to assure it is incremented. The number of values used in this test is determined by software memory requirements.

The next step 122 is a block transfer test which may be used to verify the block move function, block compare, and translate and test functions. The block move is tested by copying prestored known values into a table using the auto increment and repeat type of instructions. At the completion of this instruction registers used by the instruction are checked against known values. The values in the table are then compared against the known values stored in the table. The next instruction to be used in this test set is the translate and test instruction. This instruction is given a known string and a known table. The flags, registers and translated bits used by the instruction are then checked against known values.

During and after each of the steps 104-122, the instruction fetch, decode and other signals generated automatically by the processor are monitored by the WAM indicating the completion of a test step. At the completion of all of the above steps 102-122, the self-test next executes the step 102 in which a ticket-punch or reset signal is sent from the signal processor under test to the Watchdog Activity Monitor hardware which is expecting a ticket-punch at the precise time that the activity count reaches an expected value. If not received at this expected moment, the channel is severed by the WAM.

A fixed interval Watchdog Activity Monitor (WAM) 200 for use with a comprehensive, functionally modeled self-test of a signal processor, according to the present invention, is illustrated in FIG. 4.

The fixed interval Watchdog Activity Monitor (WAM) 200 is initialized by a synchronizing, or Macrosync (MS) signal on a line 202. The Macrosync signal is a periodic signal which is used to frame synchronize the overall system operation. It is shown as a pulse 203 occurring at a time  $t_0$  in FIG. 5(a) and recurring a fixed interval of time later at time  $t_M$ . The WAM 200 comprises a fixed count counter, but the count may be programmable. The WAM includes a control logic section 204, an eight bit register/counter section 206, a comparator 208, and WAM sever logic 210. The particular implementation of the WAM 200 shown in FIG. 4 uses a register/counter 206 for counting count signal pulses and which is preset by a load command signal on a line 244. The counter is loaded with a total count and counted down to zero by a clock signal on a line 242 which clocks in count signal pulses on a line 245 when enabled by a count enable signal on a line 246. The WAM 200 can be cleared by the processor's CPU to start operation using a CLEAR signal on a line 247.

Besides being responsive to the Macrosync and CLEAR signals, the control logic 204 is also responsive to a window signal on a line 248 which may be generated by a frequency countdown, and which, when active, indicates the allowable window of real time during

which the WAM must be legitimately started and stopped. The window may begin right after the occurrence of the Macrosync signal as shown in FIG. 5(b) by a waveform 249 which shows the window beginning at time  $t_0$  and ending at a time  $t_4$ .

The control logic 204 is also responsive to a START signal on a line 250 which may be a decoded signal generated by software to signify the start of a predetermined period of real time, i.e., the start of the timed WAM self-test sequence occurring in the signal processor. The start signal is shown beginning at time  $t_1$  in FIG. 5(c) as indicated by a signal pulse 251 which ends at a time  $t_2$ .

According to the present invention, the WAM self-test will be performed once per Macrosync period and the test will have a precise duration. Although the precise duration of each test is not specifically monitored or timed, it is effectively measured by the counter since the preplanned duration of each test is known in advance. The test must thus have a precise duration in this sense, that it must take place exactly according to the expected sequence of test state transitions which must have a duration exactly equal to a known duration, albeit only indirectly measured. As described above, it is a comprehensive test designed to exercise the major functional blocks of the processor. In the best mode implementation disclosed herein, the execution of this test is monitored by the WAM function in terms of a precise number of data and instruction fetch operations executed over a precisely known period. However, it should be understood that measures of activity other than those disclosed herein are possible and are entirely consistent with the concepts disclosed herein. In any case, each such measurable activity constitutes a state transition for the processor and is used to count down the counter 206 by means of the COUNT signal on the line 245. At the conclusion of the allotted time, the signal processor's CPU sends a RESET signal on a line 252, also known as a "ticket punch" or "keep-alive" signal, to the WAM 200 as indicated by a signal pulse 253 shown in FIG. 5(d). Since the counter 206 is preset to the total number of measured and predetermined activities in a given self-test, the occurrence of the reset pulse on the line 252 at time  $t=t_3$ , in the absence of any processor faults, must coincide with the countdown reaching zero in the counter 206. Any other combination of circumstances is indicative of a fault and leads to a power sever request signal on a line 258 as generated by the WAM Sever Logic 210. For example, if the reset pulse on the line 252 occurs before the count has reached zero or is absent when the count reaches zero, the WAM Sever Logic 210 generates a power sever request signal on the line 258.

As explained, the logical implementation of this WAM function may be accomplished by counting occurrences of a specific selected CPU activity on a line 245 in the eight bit register/counter 206 which is driven by the processor clock pulses on the line 242. Upon being initialized by the LOAD signal on the line 244 the counter 206 begins its count of CPU activities after receiving a COUNT enable signal on the line 246. The LOAD signal loads the prespecified count total and may be activated once per Macrosync frame by the WINDOW signal on the line 248 and held valid until the simultaneous occurrence of the START signal on the line 250 and the WINDOW signal on the line 248 at which time it is removed, allowing the counter to count

arm latch so that, if the processor later issues an unsever command without a POR (power or reset) or pilot request signal on a line 220 being valid (indicating a processor failure such as lost software), that incorrect action itself clears the sever latches and causes a sever. This last feature provides an added degree of enhanced processor fault coverage.

Although the invention has been shown and described with respect to a best mode embodiment thereof, it should be understood by those skilled in the art that the foregoing and various other changes, omissions, and additions in the form and detail thereof may be made therein without departing from the spirit and scope of the invention.

We claim:

1. A watchdog activity monitor (WAM) responsive to a power-on-reset signal for providing a start-up sever signal for severing selected signal processor output signals and responsive to a subsequent unsever request signal for providing an unsever signal for unsevering the selected processor output signals, the WAM for use with a signal processor repetitive self-test, the self-test having associated therewith a start signal pulse indicative of the beginning of each self-test, state transition signal pulses provided by the processor during each self-test upon the occurrence of test state transitions, and a reset signal pulse provided by the processor indicative of the conclusion of each self-test, the WAM comprising:

counter means, responsive during each repetition of the self-test to the start signal pulse from the signal processor and the state transition signal pulses for providing an output signal having a magnitude indicative of the number of state transition signal pulses received after the reception of the start signal pulse; and

sever logic means, responsive to the reset signal pulse and to said output signal for providing a sever signal for severing the selected signal processor output signals if the magnitude of said output signal is different from a selected magnitude at the time the reset signal pulse is provided.

2. The WAM of claim 1, further comprising:

independent timing means responsive to selected processor pulses for timing the interval between said selected processor pulses and providing a timing signal indicative of the duration of said interval; and

means for comparing the magnitude of said timing signal to a selected magnitude and for providing a sever signal for severing the selected signal processor output signals if said timing signal magnitude differs from said selected magnitude.

3. The WAM of claim 1, further comprising further sever logic means, responsive to a first to occur unsever request signal for providing an unsever signal for unsevering the selected output signals of the signal processor and responsive to any subsequent unsever request signals for providing a sever signal for severing the selected output signals of the signal processor.

4. The WAM of claim 1, further comprising further sever logic means responsive to a power-on-reset signal for providing the start-up sever signal for severing the signal processor output on start-up and responsive to the first to occur of any subsequent unsever request signals for providing an unsever signal for unsevering the selected output signals of the signal processor and responsive to any additional unsever request signals for

providing a sever signal for severing the selected output signals of the signal processor.

5. A watchdog activity monitor (WAM), responsive to an unsever request signal by providing an unsever signal for unsevering selected output signals of a signal processor, the WAM for use with a signal processor repetitive self-test having associated therewith a number of sub-tests, a clock signal, a repetitive frame synchronizing signal pulse and a self-test window signal for indicating a subframe within each repetitive frame within which subframe a self-test may be executed, a start signal pulse and a reset signal pulse, occurring respectively, at the beginning and end of each self-test, and the processor providing, during the course of each self-test, state transition signal pulses upon the occurrence of transitions between selected sub-test states, the WAM comprising:

logic means, responsive to the frame synchronizing pulses and the window signals for enabling a self-test sequence within each subframe, said logic means also responsive, during each subframe, to a start signal pulse from the signal processor for providing a load count signal and a count enable signal in response thereto, said logic means also responsive, during each subframe to a reset signal pulse from the signal processor for providing a reset request signal in response thereto;

counter means, responsive to said load count signal and to said count enable signal, for respectively loading a count signal magnitude and for enabling the counting of a plurality of state transition signal pulses during each subframe, said counter means also responsive to the state transition signal pulses and the clock signal from the processor for counting upon each simultaneous reception of both a clock signal pulse and an edge of the state transition pulse within a subframe, said counter means providing a counted output signal having a magnitude indicative of the number of state transition signals received during the subframe; and

means responsive to said reset request signal and to said counted output signal for comparing, at the time said reset request signal is received, the magnitude of said counted output signal to a reference signal having a magnitude indicative of the magnitude of the number of selected sub-test states and for providing a sever signal for severing the selected output signals of the signal processor if said counted output signal magnitude differs from said reference signal magnitude.

6. The WAM of claim 5, wherein said logic means further comprises means for comparing the sequence of received window, start, and reset signals within each repetitive frame to a selected expected sequence and for providing a sever request signal in the presence of a received signal sequence different from the selected expected sequence.

7. The WAM of claim 5, further comprising:

independent timing means, responsive to selected signal pulses from the processor for measuring a time interval between said selected processor signal pulses and providing an interval signal indicative of the duration of said interval; and

means for comparing the magnitude of said interval signal to a time reference signal having a magnitude indicative of the duration of each frame and for providing a sever signal for severing the selected signal processor output signals in the pres-

UNITED STATES PATENT AND TRADEMARK OFFICE  
CERTIFICATE OF CORRECTION

PATENT NO. : 4,727,549

DATED : 2/23/88

INVENTOR(S) : Bhalchandra R. Tulpule et al

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Claim 1, column 13, lines 40-41.

Cancel the second occurrence of  
"signals" and substitute -- signal --

Claim 4, column 13, line 68.

After "signals" insert  
-- occurring after said first to  
occur unsever request signal --

Claim 5, column 14, line 24.

Cancel "siad" and substitute  
-- said --

Claim 10, column 16, line 8.

Cancel "reptiition" and substitute  
-- repetition --

Claim 12, column 16, line 31.

Cancel "porcessor" and substitute  
-- processor --

Signed and Sealed this  
Twenty-fourth Day of January, 1989

*Attest:*

DONALD J. QUIGG

*Attesting Officer*

*Commissioner of Patents and Trademarks*

BEST AVAILABLE COPY